Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Computing Security Algorithm

Rachna Jain, Ankur Aggarwal
Bharati Vidyapeeth's College Of Engineering,
Guru Gobind Singh Indraprastha University, India

Abstract— This paper elucidates a security model that can be implemented for a Cloud computing infrastructure, which can ensure security at top level of architecture while maintaining the integrity of the system. The data encrypted by the proposed algorithm will only allow data file to open in the computer where it was used to encrypt. Cloud Computing is rapidly increasing technology that is witnessing ever expanding implementation in already existing network architecture. For it to hit with no loopholes or giving away any opportunity to hackers we need to ensure that it has highest security algorithm working behind it.

Keywords— Cloud Computing, Security ,RSA,AES,MD5

I. INTRODUCTION

In any network based model there comes a necessity to implement a security algorithm that not only can keep the data safe from external interference but also keep the Data intact and easy to decrypt in a time little than long. Every major companies like Google, Apple, Amazon' S3 offer their client with cloud storage service. All professional industries are using Cloud Computing model at various levels with business model like Paas (Platform-as-a-Service), Iaas (Infrastructure-as-a-service), Saas (Software-as-a-service) and Haas (Hardware-as-a-service) distributed to various end users. This paper gives few already proposed algorithms with their drawbacks and tries to eliminate those from our proposed algorithm.
Currently there are three types of Clouds: Private, Public and Hybrid.
The next section explains the different algorithms already at play.

Cloud Computing Security Models

1.Identity-based cryptography

Identity-based cryptography is a public key technology that allows the use of a public identifier of a user as the user's public key. Hierarchy identity-based cryptography is the development from it in order to solve the scalability problem. Recently identity-based cryptography and hierarchy identity-based cryptography have been proposed to provide security for some Internet applications.

2.RSA

It is an algorithm for public-key cryptography. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. This algorithm finds its application in Cloud Computing. This involves a public key and a private key. The public key is known to everyone on a network and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key, which is available at the receivers end, allowing only him to decrypt the message.

3.MD5

Message-Digest algorithm 5 (MDA 5), a widely used cryptographic hash function producing a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks. The message is padded so that its length is divisible by 512.[]
In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

4.AES

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes

- 128-bit keys for 10 cycles of repetition.
- 192-bit keys for 12 cycles of repetition.
- 256-bit keys for 14 cycles of repetition.

AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper. AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware.

II. CLOUD COMPUTING CONCERNS

Every Cloud service faces a security concern in many different ways as to how the data can be leaked in a network during its transmission or storage. There are many security concerns like:

Availability of Data:
Is the data available for its storage and its location. This will ensure access to data whenever it's asked for.
Encryption:
What type of cloud whether public, private or hybrid, decides the type of encryption standard that will be used. The security of data has to be ensured by the service providers by following a set standard.
Data Integrity:
When the data is stored in a place other your computer like in a cloud, data may be stored at different places scattered in the whole storage. When accessing the data the service providers must ensure the data integrity while delivering back the data from their storage.

III. Proposed Algorithm

The following algorithm eliminates the need to share any password and lets user to open the files stored in the cloud specifically to the computer in which it was used to store at the first place. The main idea behind is to use the identification of the computer over the network as the security key, which will be used to encrypt the data. All the encryption will be done on the client's side. Hence it makes no data readable on the network or the service provider giving it utmost level of security. The following algorithm will allow users to save data over the Internet without fearing any data theft. The interface can be made for the method, which will make a random key and attach an id number, which will be stored locally on the computer. This id will be sent with the data in the storage. Whenever the data will be used to access it over the network you will have to unpack the data using the same interface and it will use the id sent with the data and locate the id and mapped key with that id locally on the computer and decrypt it. The key size and the key itself can be randomized. The advantage of this technique is that the data can be accessed from either a secure or unsecured network allowing users to save their data over the network while having the key with them.
Different devices can be synchronized with the computer through the interface software and these devices will then be able to get the table made according to the scheme of randomization used to make the id and the key. Then this one time synchronization will last forever. The scheme generated will be randomly selected for the storage of the keys and their ids.
Key generation will be done on each device every time a new data is wished to put on network. This will ensure that the devices are kept in synchronization. And keys will be generated on every device separately.

IV. Advantage of the proposed algorithm

- No key shared over the network while maintaining the data encrypted over the network.
- No data integrity lost
- Data cant be spoofed between the network.
- Total security of the data no matter which network (private or public) you use to access the data.
- Data cannot be decrypted by any technique for no information will be made available about the key size.
- Brute force can also not be used for the above reason.

The only drawback this algorithm/scheme sees is the need to synchronize the devices on initial setup. But this makes the need to make the data secured with a hardware lock of physical need to synchronization of data.

V. Conclusion

In this paper we design an algorithm which ensures utmost data security to users to as many devices he wish to have the data captured from the network. The initial synchronization of the devices lets the software know the devices it can share the key data with. Keys will be generated separately on each device and hence the synchronization will be ensured.

REFERENCES

[1] K.S.Suresh, K.V.Prasad "Security Issues and Security Algorithms in Cloud Computing", published in International Journal of Advanced Research in Computer Science and Software Engineering, October 2012.
[2] Jenny Torres, Michele Nogueira, Guy Pujolle "Identity-Based Cryptography: Applications, Vulnerabilities and Future Directions", published in IGI global.
[3] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", in 2010 IEEE.
[4] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues", in 2010 IEEE.
[5] Gartner. "Seven cloud-computing security risks". http://www.infoworld.com July 02,2008.
[6] http://en.wikipedia.org/wiki/Cloud_computing.
[7] Elinor Mills, January 27,2009. "Cloud computing security forecast: clear skies".
[8] Farzad Sabahi, "Cloud Computing Security Threats and Responses", in 2011 IEEE.
[9] Liang Yan, Chunming Rong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography", in Springer-Verlag Berlin Heidelberg 2009.
[10] Mandeep Kaur, Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing", in International Journal of Communication and Computer Technologies, January 2013.

